UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/667,286	09/22/2000	Magda M. Mourad	(YOR920000599)13873	1205

7590 01/03/2006

Richard L Catania
Scully Scott Murphy & Presser
400 Garden City Plaza
Garden City, NY 11530

EXAMINER
TRUONG, THANHHGA B

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/667,286	**Applicant(s)** MOURAD ET AL.
	Examiner Thanhnga B. Truong	**Art Unit** 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/3/2005 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 July 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) ☐ Notice of Informal Patent Application (PTO-152)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.	6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on October 3, 2005 has been entered. Claims 1-21 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-16, 18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ram et al (US 6,519,700 B1), and further in view of Vandergeest (US 6,247,127 B1).

a. <u>Referring to claim 1:</u>

i. Ram teaches:

(1) a verification system (e.g. a rights enforcer) to validate the integrity of the player applications, and including a certificate generator for generating a certificate after inspecting the player application code and determining that a certain required property has been met by said code **[i.e., a rights enforcer 524 is present to verify the user's identity, to compare a requested action by the user to those actions enumerated in the rights and permissions segment 514, and to permit or deny the requested action depending on the specified rights (column 8, lines 37-41)];**

(2) a trusted content handler (e.g. a user system) to decrypt content and to transmit the decrypted content to the player applications, using an extension mechanism defined by the application, and to enforce usage rights associated with the content **[i.e., referring to Figure 1, the user 118 is then able to use his private key to decrypt the modified content 116 and view the original content 112 (column 6, lines 6-14). In addition, Figure 3 looks similar to FIG. 2, in that an encrypted document 310 is passed to a decryption step 312 (which uses a**

private key 314) and a rendering application 316, resulting in presentation data 318 (column 6, lines 3-6)]; and

(3) a user interface control module (e.g., a rights and permission segment) to ensure that the user interaction with the player applications does not violate the usage rights **[i.e., a rights enforcer 524 is present to verify the user's identity, to compare a requested action by the user to those actions enumerated in the rights and permissions segment 514, and to permit or deny the requested action depending on the specified rights (column 8, lines 37-41). In addition, the rights and permissions segment 514 is cryptographically signed (by methods known in the art) to prevent tampering with the specified rights and permissions; it may also be encrypted to prevent the user from directly viewing the rights and permissions of himself and others (column 8, lines 23-27)]**;

(4) wherein components of the verification system, the trusted content handler, and user interface control module of the digital rights management system operate independently from the player application and reside locally in an end-user device having said player applications **[i.e., the portions of the invention described in Ram's system that are described as software components could be implemented as hardware. Moreover, while certain functional blocks are described herein as separate and independent from each other, these functional blocks can be consolidated and performed on a single general-purpose computer, or further broken down into sub-functions as recognized in the art. (column 14, lines 5-12)]**.

i. Ram teaches the user's certificate as shown in column 11, line 4 and lines 30-31, however Ram does not explicitly mention a certificate generator for generating a certificate after inspecting the player application code and determining that a certain required property has been met by said code. On the other hand, Vandergeest teaches:

(1) To ensure that the receiving party is using an authentic public key of the sending party, it obtains a signature public key certificate from the directory or a certification authority. The signature public key certificate

includes the signature public key of the sending party and the signature of the certification authority. After obtaining the certificate, the receiving party first verifies the signature of the certification authority using a locally stored trusted public key of the certification authority. Once the signature of the certification authority has been verified, the receiving party can trust any message that was signed by the certification authority. Thus, the signature public key certificate that the receiving party obtained is verified and the signature public key of the sending party can be trusted to verify the signature of the sending party of the message **(column 1, lines 52-67 of Vandergeest).** Furthermore, referring to Figure 1, Vandergeest teaches the certification authority 22 performs policy control for the communication system, which includes generating encryption and signature public key certificates, establishing cross certificates, etc **(column 3, lines 34-37 of Vandergeest).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include the certificate generator and repository in Ram's SPD system for protection during document delivery from a document distributor to an intended user over a public network, as well as during document storage on an insecure medium **(column 2, lines 17-20 of Ram).**

iv. The ordinary skilled person would have been motivated to:

(1) include the certificate generator and repository in Ram's SPD system since certain trusted components can be deployed, one must continue to rely upon various unknown and untrusted elements and systems. On such systems, even if they are expected to be secure, unanticipated bugs and weaknesses are frequently found and exploited **(column 2, lines 37-41 of Ram).**

b. *Referring to claim 4:*

i. Ram further teaches:

(1) wherein the player applications request protected content, and the trusted content handler includes an authenticator to verify that a player application that requests protected content has been authorized by the verification system to access the requested, protected content **[i.e., the operation performed**

when a user receives an SPD are depicted in the flow diagram of Figure 7. The SPD is first received and stored at the user's system (step 710); in many usage, it is not necessary to use the SPD right away. When usage is desired, the user is first authenticated ..... as discussed above (column 12, lines 11-32)].

c. *Referring to claim 5:*

i. Ram further teaches:

(1) wherein a user interface control module traps user interface related messages generated as a result of user interactions with player applications, blocks messages that lead to usage rights violations, and passes through other messages to the player applications **[i.e., the generic SPD 610 is received by the distributor 114, and is stored for later customization. When a user request 624 is received by the distributor 114 (either directly or through the clearinghouse 122 or other intermediary), the distributor 114 creates a set of user permissions (step 626) that is consistent with both the user request 624 and the rights specification 614. If there is no such consistent set of permissions, then no further action is performed on that user's behalf (other than an optional notification message to the user) (column 11, lines 47-56)].**

d. *Referring to claims 6 and 10:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

e. *Referring to claims 9 and 13:*

i. These claims have limitations that is similar to those of claim 4, thus they are rejected with the same rationale applied against claim 4 above.

f. *Referring to claim 2:*

i. Ram teaches the claimed subject matter, however Ram does not explicitly mention an off line verifier to verify that the player applications have certain properties, and to issue trust certificates to verify that the player applications have said properties. On the other hand, Vandergeest teaches:

(1) The secure information includes the certificates of end-users, or targeted communication entities. While the off-line end-user may receive

the certificates for all other end-users of the system, typically, the off-line end-user will only request the certificates of end-users of interest, i.e., ones that will be involved in a secure communication with the off-line end-user. The secure information may further include cross-certificates 38, an authority revocation list 38, and a certificate revocation list 40. The off-line end-user verifies the secure information by comparing a time stamp of the security information with a validity period, which is based on the frequency at which the revocation lists 38 and 40 are updated. Thus if the revocation list 38 and 40 are updated daily, the validity period is 24 hours. The off-line end-user may further verify the security information by ensuring that a trust party (e.g., a trusted certification authority) signed the security information and the trusted party is not identified on the authority revocation list. The off-line end-user may still further verify the security information by determining that certificate of the at least one targeted communication is not on the certificate revocation list. The off-line end-user may even further verify the security information by ensuring that appropriate key usage, i.e., encryption keys are used for encryption purposes and verification keys are used for verification purposes. The off-line end-user may still even further verify the security information by ensuring policy compliance regarding the security information and messages based thereon **(column 4, lines 45-66 of Vandergeest).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly disclose a certificate generator in Hurtado for providing off-line secure communication **(column 2, lines 51-52 of Vandergeest).**

iv. The ordinary skilled person would have been motivated to:

(1) include the off-line verification to allow end-users to go off-line from a security information repository (e.g., a directory, a certification authority, or a server), and confidently participate in secure communications. As such, an end-user, while off-line, may securely and in a trustworthy manner, read encrypted e-mail messages, prepare secure outgoing messages, access encryption protected folders, etc **(column 3, lines 3-9 of Vandergeest).**

g. _Referring to claim 3:_

i. Ram further teaches:

(1) wherein the verification system further includes a verifying launcher for verifying that a particular player application is certified as a trusted application before digital content is transmitted to said particular player application **[i.e., enforcement of rights and verification of conditions associate with rights is performed using the SPD (self-protecting-document) technology (column 10, lines 2-4). The generic SPD 610 is created by combining the pre-processed content 612, the pre-processed rights specification 614, and the watermark 616. A watermark may be added by any means known in the art; it may be either visible or concealed within the SPD. The generic SPD 610 may also optionally be encrypted by the author/publisher 110 for transmission to the distributor 114 as shown in Figure 1 (column 11, lines 39-46)].**

h. *Referring to claims 7 and 11:*

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

i. *Referring to claims 8 and 12:*

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

j. *Referring to claim 14:*

i. This claim has limitations that is similar to those of claims 1 and 2, thus it is rejected with the same rationale applied against claims 1 and 2 above.

k. *Referring to claim 15:*

i. Ram further teaches:

(1) wherein the code verifier is responsible for launching the player application and verifying the identity and integrity of the code using the information in the trust certificate before launching the application; the launch procedure returning process identification information, which the code verifier records internally; the authenticator communicating the same or other process identification information concerning its own process, which it obtains from system service calls, to the code verifier at the time the application requests: content from the authenticator; the code

verifier matching this process identification information against the process identification information it recorded; the code verifier returning a code indicating whether the process was verified or not **[i.e., the self-protecting document 510 includes three major functional segments: an executable code segment 512 contains certain portions of executable code necessary to enable the user to use the encrypted document; a rights and permissions segment 514 contains data structures representative of the various levels of access, that are to be permitted to various users; and a content segment 516 includes the encrypted content 116 (FIG. 1) sought to be viewed by the user (column 7, lines 52-60). A secure viewer 530 is optionally included in the executable code segment 512. The secure viewer 530 is used to permit only those levels of access that are permitted according to the rights and permissions segment 514. For example, if the user purchased only sufficient rights to view a document (and not to save or print it), the viewer will not permit the user to save, print, or perform the standard cut-and-paste operations possible in most modern operating systems (column 9, lines 8-15)].**

l. *Referring to claim 16:*

i. This claim has limitations that is similar to those of claim 15, thus it is rejected with the same rationale applied against claim 15 above.

m. *Referring to claims 18 and 20:*

i. These claims have limitations that is similar to those of claim 14, thus they are rejected with the same rationale applied against claim 14 above.

4. Claims 17, 19, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ram et al (US 6,519,700 B1), further in view of Vandergeest (US 6,247,127 B1), and further in view of Peinado (US 6,775,655).

a. *Referring to claim 17:*

i. The combination of teachings between Ram and Vandergeest teaches the user's certificate as shown in column 11, line 4 and lines 30-31 of Ram; and Vandergeest teaches, as shown in Figure 1, the certification authority 22 performs policy control for the communication system, which includes generating encryption and signature public key certificates, establishing cross certificates, etc (column 3, lines 34-37 of Vandergeest). Vandergeest further teaches:

(1) wherein the trust certificate includes: a program identifier identifying said one of the applications; a property name identifying an attribute certified by the trust certificate; a code digest of the one application; a digital signature containing a secret key of the application certifier; and a certifier identification containing a public key of the application certifier **[i.e., the certificates 34 each include a public key of a particular end-user in the communication system. Each certificate 34 also includes a signature of a certification authority. When a user receives the certificate, it verifies the signature of the certification authority and once verified, can confidently use the public key of the end-user to encrypt and/or verify signatures of the end-user identified in the certificate. The cross-certificates 36 each include the signature key of a certification authority and the signature of a trusted certification authority. With a cross-certificate, an end-user may use the signature of another certification authority 3 to verify certificates signed by the another certification authority. This can only be done if a trusted certification authority signs the cross certificate. The authority revocation list 38 indicates which certification authorities have lost their status as a certification authority. In other words, the authority revocation list 38 indicates which certification authorities' signatures can no longer be trusted. The certificate revocation list 40 includes a list of end-users whose certificates have been revoked (column 3, lines 46-65 of Vandergeest)].**

ii. However, Ram and Vandergeest do not explicitly mention the identification of the certificate. On the other hand, Peinado teaches:

(1) The public key of the black box 30 of the DRM system 32 (PU-BB); the version number of the black box 30 of the DRM system 32; a certificate with a digital signature from a certifying authority certifying the black box 30 (where the certificate may in fact include the aforementioned public key and version number of the black box 30); the content ID (or package ID) that identifies the digital content 12 (or package 12p); the key ID that identifies the decryption key (KD) for decrypting the digital

content 12;) **(column 18, lines 60-67 through column 19, lines 1-4 of Peinado).** Furthermore, the certificate with the digital signature from the certifying authority, also discussed above in connection with the license acquisition function, is a proffer or vouching mechanism from the certifying authority that a license server 24 should trust the black box 30. Of course, the license server 24 must trust the certifying authority to issue such a certificate for a black box 30 that is in fact trustworthy. It may be the case, in fact, that the license server 24 does not trust a particular certifying authority, and refuses to honor any certificate issued by such certifying authority. Trust may not occur, for example, if a particular certifying authority is found to be engaging in a pattern of improperly issuing certificates **(column 22, lines 36-48 of Peinado).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include the certificate identification in Ram's SPD system for protection during document delivery from a document distributor to an intended user over a public network, as well as during document storage on an insecure medium **(column 2, lines 17-20 of Ram).**

iv. The ordinary skilled person would have been motivated to:

(1) include the certificate identification in Ram's SPD system since certain trusted components can be deployed, one must continue to rely upon various unknown and untrusted elements and systems. On such systems, even if they are expected to be secure, unanticipated bugs and weaknesses are frequently found and exploited **(column 2, lines 37-41 of Ram).**

b. <u>*Referring to claims 19 and 21:*</u>

i. These claims have limitations that is similar to those of claim 17, thus they are rejected with the same rationale applied against claim 17 above.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

KIM VU
PATENT EX
CENT

TBT
December 20, 2005